524 TECHNOLOGY AND INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies; including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

V. UNACCEPTABLE USES

A. The following uses of the school district system, devices, and Internet resources or accounts are considered unacceptable:

1. Users will not use the school district system or devices to access, review, upload, download, store, print, post, receive, transmit, or distribute:

a. pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;

b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

d. information or materials that could cause damage or danger of disruption to the educational process;

e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the school district system or devices to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

3. Users will not use the school district system or devices to engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use the school district system or devices to vandalize, damage, or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means, will not tamper with, modify, or change the school district system software, hardware, or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

5. Users will not use the school district system or devices to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

6. Users will not use the school district system or devices to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone

numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not re-post a message that was sent to the user privately without permission of the person who sent the message.

a. This paragraph does not prohibit the posting of employee contact information on school district web pages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

b. Employees creating or posting school-related web pages may include personal contact information about themselves on a web page. However, employees may not post personal contact information or other personally identifiable information about students unless:

(1) such information is classified by the school district as directory information and verification is made that the school district has not received notice from a parent/ guardian or eligible student that such information is not to be designated as directory information in accordance with **Policy 515; or**

(2) such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with **Policy 515**.

In addition, prior to posting any personal contact or personally identifiable information on a school-related web page, employees shall obtain written approval of the content of the postings from the building administrator.

c. These prohibitions specifically prohibit a user from utilizing the school district system or devices to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "MySpace" and "Facebook."

7. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system or devices, attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the school district system or devices to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

9. Users will not use the school district system or devices for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement without authorization from the appropriate school district official.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet or devices when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VI. FILTER

A. With respect to any of its devices with Internet access, the school district can monitor the online activities of both minors and adults and employ technology protection measures during any use of such devices by minors and adults. The technology protection measures utilized are designed to block, monitor and filter Internet access to any visual depictions that are:

1. Obscene;
2. Child pornography; or
3. Harmful to minors.

B. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

C. The school district will inform students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the school district system or devices and use of the Internet shall be consistent with school district policies and the mission of the school district.

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).

F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

IX. TECHNOLOGY AND INTERNET USE AGREEMENT

A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents, and employees of the school district.

B. This policy requires the permission of the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet Use Agreement form for students must be read and signed by the user, and the parent or guardian. The Internet Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office.

X. Wireless Connectivity/Personal Devices

A. Personal laptop and Internet-enabled handheld devices can be used on the wireless network of the district solely for academic and instructional purposes. Students must meet the expectations stated below to protect the school network as well as their personally owned devices. These devices include, but are not limited to, laptops, netbooks, iPods, iPads, iPhones, Blackberrys, or any Internet-enabled device.

B. Wireless Internet-enabled devices may be used as determined by building protocol. Students who are not doing academic work, or are creating a disruption, will be asked to put the device away. Students must ask permission of each individual teacher to use the device during an academic class.

C. The district maintains a wired network to secure administrative and instructional functions. The district also maintains a wireless public network. Both networks are filtered for acceptable content. The student network accounts are only available from wired school computers.

D. Expectations

1. The student/owner must have a signed AUP and follow all conditions and acceptable uses of the Internet as outlined in the district Acceptable Use Policy.

2. The owner of the device is solely responsible for the physical security and the network security of the device, including virus protection, even when shared/loaned to another student.

3. The owner is solely responsible and capable of setting up the device on the network and provides all necessary equipment such as battery, power supply, and connections.

4. Student-owned devices should only be connected to the guest network, and NEVER be connected to the district's wired network, or any other wireless network in the district.

5. With permission of a teacher, students may charge their device in an academic room.

6. School staff will NOT provide technical support and peripheral support.

XII. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on school district diskettes, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school

district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XIII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Technology and Internet use.

B. This notification shall include the following:

1. Notification that Technology and Internet use is subject to compliance with school district policies.

2. Disclaimers limiting the school district's liability relative to:

a. Information stored on school district diskettes, hard drives, servers, devices or cloud-based servers.

b. Information retrieved through school district computers, networks, or online resources.

c. Personal property used to access school district computers, networks, or online resources.

d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.

6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 55, Protection and Privacy of Pupil

7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

Legal References:

15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act)

17 U.S.C. § 101 et seq. (Copyrights)

20 U.S.C. § 6751 et seq. (Enhancing Education through Technology Act of 2001) 47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA)) 4'7 C.F.R. 54.520 (FCC rules implementing CIPA)

Minn. Stat. § 121A.0695 (School Board Policy; Prohibiting Intimidation and Bullying)

Minn. Stat. l25B.l5 (Internet Access for Students) Minn. Stat. 125B.26 (Telecommunications/ Internet Access Equity Act)

Tinker v. Des Moines Indep. Cmty. Sch. Dz'st., 393 US. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)

United States v. Amer. Library Assoc, 539 US. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)

Doninger" v. 527 F.3d 41 Cir. 2008)

La)/shock v. Hermimge Sch. Dist, 412 F.Supp.2d 502 (W.D. Pa. 2006) MT v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007) .].S. v. Bethlehem Area Sch. Dist, 807 A.2d 847 (Pa. 2002)

Cross References:

MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)

MSBA/MASA Model Policy 406 (Public and Private Personnel Data)

MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)

MSBA/MASA Model Policy 506 (Student Discipline)

MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records) MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies) MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination) MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination) MSBA/MASA Model Policy 603 (Curriculum Development) MSBA/MASA Model Policy 604 (Instructional Curriculum) MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials) MSBA/MASA Model Policy 806 (Crisis Management Policy)

MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)